STRATEGY
RESEARCH
PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

INFORMATION WARFARE IN THE CYBER DOMAIN

BY

COLONEL GLENN H. TAKEMOTO
United States Army

USAWC CLASS OF 2001

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

INFORMATION WARFARE IN THE CYBER DOMAIN

by

COL GLENN H. TAKEMOTO
Department of the Army

Professor Malcolm C. Cowley
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: COL Glenn H. Takemoto

TITLE: Information Warfare in the Cyber Domain

FORMAT: Strategy Research Project

DATE: 26 February 2001 PAGES: 34 CLASSIFICATION: Unclassified

Information technology is rapidly advancing, particularly in the Cyber Domain. As our reliance on this technology increases, so too does our vulnerability in terms of national security. This corollary makes it imperative that we develop optimal operational doctrine for Information Warfare in the Cyber Domain (IWCD).

This paper lays a foundation by defining the terminology associated with Information Warfare in the Cyber Domain, reviews the threat and illustrates the vulnerabilities of our information systems, discusses our nation's policies and efforts to wrestle with the growing problem of information security, and traces the subject of information security through our National Security Strategy (NSS), our National Military Strategy (NMS), Department of Defense (DoD) Directives, Joint Vision 2020, and our Joint doctrine.

Following the background information, we present an example of a possible approach for doctrinal development that takes the nine principles of war, integrates the USAF's doctrinal interpretation of each principle and synthesizes them into principles for IWCD. This example is rooted in the nine fundamental principles of war, Air Force doctrine, and three new premises for Information Warfare in the Cyber Domain. These three new premises are: 1) establishment of **cyber supremacy is essential** for operational success, 2) IWCD can be **the** weapon of choice for future decision-makers, and 3) IWCD can **itself** bring about conflict resolution in certain situations. Lastly, we look at some examples of how to employ these synthesized principles and three new premises of IWCD in operational doctrine.

Doctrinal development must be made a top priority. This paper presents an example of ***a*** possible approach to further doctrinal development using the nine principles of war as a framework. There are many other methods. The intent is to spur further thought and progress towards developing ***the*** correct doctrine for our nation. New approaches, paradigms, and doctrine are required to allow our control and unrestricted use of this new medium in order to achieve tactical, operational, and strategic objectives and ultimately ensure our national security.

TABLE OF CONTENTS

Information Warfare in the Cyber Domain

Information technology is rapidly advancing, particularly in the Cyber Domain. As our reliance on this technology increases, so too does our vulnerability in terms of national security. This corollary makes it imperative that we develop optimal operational doctrine for Information Warfare in the Cyber Domain (IWCD). Joint Pub 1-02 **defines doctrine as**: "Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives."[1]

Although advances in technology continue to change warfare, our national security cannot rest on merely developing and possessing the latest technology. Technological advancement is only the first step towards ensuring our national security. Ultimately, it is the human being who determines how to apply the technology to its maximum potential. Man harnesses the doctrine by using the "ways" of imagination, innovation, initiative, and ingenuity, and combining them with the "means" provided by the technology, to achieve the desired "end" of ensuring our national security. The key is to determine how to gain the greatest advantage of this new potential by developing and applying ***the*** correct doctrine. **Joint Vision 2020 states**:

> "Materiel superiority [new technology] alone is not sufficient. Of greater importance is the development of doctrine, organizations, training and education, leaders, and people that effectively take advantage of the technology."[2]

We place our national security at risk if our vision is faulty, i.e., if we fail to recognize change; fail to actively learn, adapt, and anticipate; fail to develop the technology; and fail to develop the doctrine necessary to correctly employ technology in light of change.

Historically, combatants who recognized a changing environment, correctly divined the implications and impacts of technological changes, and subsequently developed and applied the correct doctrine, were proven successful on the battlefield. A 20th Century example of failure in this critical dynamic between a changing environment, new technology, and doctrinal development was the Battle of France in the early days of World War II. It took only a matter of weeks, from the German Airborne assault into France on 10 May 1940 to their victory march down the Champs-Elysees on 14 June 1940, to graphically illustrate the penalty for failure and its catastrophic impact on national survival. In the years preceding May 1940, both the French and the Germans possessed the technological knowledge and equipment associated with mechanized ground forces and combat aircraft. The Germans were able to successfully develop and apply the correct doctrine to maximize the potential of the new technology in a new environment, and the French were not. The price for the French lack of vision and resulting doctrinal failure was their national sovereignty. [3] Given the rapid pace of technological advancement, and our growing dependency on technology, we cannot afford to place our nation at such risk.

Here are two views that serve to illustrate the current, **traditional view of Information Warfare**:

> 1) "The fundamentals of information warfare - affecting an adversary's information and information-based systems and defending one's own - have not changed through time. What has changed is the means and route of attack." GEN Michael Ryan, Air Force Chief of Staff[4]
>
> 2) "Information has been at the core of military operations through the ages. Throughout history, leaders have recognized the key role of information as a contributor to victory on the battlefield. Commanders have always sought - and sometimes gained - a decisive information advantage over their adversaries."
>
> "Sun Tzu's and Clausewitz's insights on information in war are timeless because war has been and continues to be a violent clash of wills between determined adversaries. A clash conducted across the dimensions of force, space, and time. A clash where the role of information has increased in importance and complexity as warriors have extended the limits of the physical domains of war from land and sea to air, space, and finally, to cyberspace."[5]

These views are still relevant. The military's desire to obtain and manage information and to use information to gain the advantage over its adversaries is not new.

The change, the newness, is in the technological means that are being developed. Great advancements have been made in computing power, communications systems, and the global interconnectivity of these systems. When most think about these new technological means, it is in terms of the new capabilities they bring.

However, there is also change and newness in the implications of these capabilities that allow the expansion of our battlespace beyond the domains of land, sea, and aerospace into the cyber domain. Looking back in history, we have used the capabilities of ships and aircraft to take us to the new domains of sea and aerospace. In order to prevail in those battlespaces, we required new doctrinal thinking. It was the new doctrine that harnessed the sea and aerospace technological capabilities, generated sea and aerospace power, allowed our control and unrestricted use of these mediums to achieve our objectives, and thus contributed to the security of our nation. We must now do the same for Information Warfare in the Cyber Domain.

Methodology.

The methodology of this paper is to first lay a foundation of background information by defining the terminology associated with Information Warfare in the Cyber Domain, reviewing the threat and illustrating the vulnerabilities of our information systems, discussing our nation's policies and efforts to wrestle with the growing problem of information security, and tracing the subject of information security through our National Security Strategy (NSS), our National Military Strategy (NMS), Department of Defense (DoD) Directives, Joint Vision 2020, and our Joint doctrine.

Following the background information, we'll present an example of a possible approach for doctrinal development. This example will be rooted in the nine fundamental principles of war, Air Force doctrine, and three new premises for Information Warfare in the Cyber Domain.

Background.

Before we can begin any discussion of information warfare, we need to define the terminology associated with information operations. Joint Pub 3-13, Joint Doctrine for Information Operations, provides these **definitions**:[6]

Computer Network Attack:

"Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."

Information Assurance:

"Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."

Information Operations:

"Actions taken to affect adversary information and information systems while defending one's own information and information systems."

Information Superiority:

"The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."

Information System:

"The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information."

Information Warfare:

"Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries."

There are currently no Joint doctrinal definitions for the cyber domain (or cyber space) and Network Centric Warfare. This paper's **definition of the Cyber Domain is**: ...the integrated and interlinked network of information, information systems, computers, advanced telecommunications, the Internet, and their respective physical support structures. The intent of this definition is to convey the idea that the cyber domain encompasses not only the physical realm, as does Information Systems, but considers the cyber medium to be on par with the domains of land, sea, and aerospace.

This paper's working definition of **Network Centric Warfare** is from the 1999 book "Network Centric Warfare."[7]

> "We define NCW [Network Centric Warfare] as an information superiority-enabled concept of operation that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace."

Currently, no definition of Information Warfare in the Cyber Domain exists. Therefore, based on the preceding doctrinal definitions, and for the purpose of this paper, our **baseline definition of Information Warfare in the Cyber Domain will be:** "Operations, to include Information Operations, conducted primarily through, but not limited to, Information Systems to gain Information Superiority and Assurance in order to achieve tactical, operational, and strategic objectives."

This definition of IWCD is a departure from the doctrinal definitions of Information Operations, Information Warfare, Information Superiority, and Information Assurance as published in Joint Pub 3-13 and from the above definition of Network Centric Warfare. This new definition of IWCD is a paradigm shift, a new way of thinking about Information Warfare. Specifically, there are at least **three new premises for IWCD**:[8]

1) Establishment of **cyber supremacy is essential for success** in future military operations. Just as air supremacy is a necessary pre-condition to successful surface operations, establishment of cyber superiority or supremacy must be viewed as a necessary pre-condition to overall success.

2) IWCD can be ***the*** offensive weapon of choice for the National Command Authority and operational commanders. Unlike Network Centric Warfare which is a "concept of operation" to use information superiority as an enabler to leverage decisive systems in the generation of combat power, IWCD is not limited to an enabling function.

3) IWCD can itself bring about conflict resolution in certain situations. IWCD operations not only support decisive operations but can also be ***the*** decisive operation for a campaign.

Now that we have defined information warfare and its associated concepts, the next step is to review the threat and illustrate the vulnerabilities of our information systems. Along with the emergence and proliferation of automated and inter-connected information systems and their increased capabilities, come new security vulnerabilities and perpetrators willing to exploit these vulnerabilities.

Winn Schwartau, a noted author on information security since 1984[9] and author of the book Cybershock, published in 2000, is a government consultant who has provided congressional testimony on the subject of information security. Schwartau defines the information security threat as virtually anything that can impede, disrupt, or destroy our ability to protect and preserve our nation. Some of his specific examples of such attacks include: denial of service, theft or destruction of data, manipulation of data, ruses and hoaxes, viruses, system slow-downs, false or deceptive information, electronic eavesdropping, and actual destruction of infrastructure.

Schwartau characterizes the threat as anyone with a computer and access to the cyber domain. Given this definition, the threat can include, but is not limited to,: persons internal to organizations, recreational hackers, criminals (both organized and individual), terrorists, industrial spies and saboteurs, multinational corporations, traditional nation states, and supra-national organizations. The target of the threat can be any organization (e.g., government, military, business, financial, public utility, transportation) or individual that would be adversely impacted by theft, manipulation, disruption, or destruction of anything reliant, connected to, or affected by an information system. Schwartau sums up our current situation and general vulnerability by stating:

> "..our reliance upon the cyber-infrastructure now exceeds our ability to live without it. But we screwed up. We built electronic highways without a means to protect them. We didn't build security in from the ground up..."[10]

Validation of Schwartau's vulnerability assessment and our lack of preparation in the cyber domain is evidenced in the results of two separate, unclassified, open source events: ELIGIBLE RECEIVER 97 and SOLAR SUNRISE.[11,12]

The results of the DoD Exercise **ELIGIBLE RECEIVER 97**, conducted 9-13 June 1997, illustrated that hostile forces could penetrate defense networks and affect the DoD's ability to perform certain missions.[13] Computer systems were disrupted by actual attacks on information systems through exploitation of known vulnerabilities. Computer networks were penetrated, services denied, emails manipulated, and phone services affected. Some of the targets were the National Military Command Center, U.S. Pacific Command, U.S. Space Command, U.S. Transportation Command, and U.S. Special Operations Command.[14,15] ELIGIBLE RECEIVER 97 demonstrated in stark fashion the vulnerability of our systems in the cyber domain, our inability to detect and assess cyber attacks, and the lack of preparation of DoD to wage Information Warfare in the Cyber Domain.

SOLAR SUNRISE was the code name given to a series of intrusions into the DoD systems and networks that occurred 1-26 February 1998. The attacks coincided with U.S preparations for potential military action aimed at Iraq over disputes on U.N. weapons inspections. During this period, Air Force, Navy, and Marine Corps computers were penetrated and sustained at least 11 attacks worldwide. The perpetrators were found to be two California teenagers and one Israeli teenager. The level of sophistication, the associated affects of the attacks, and the vulnerability of the DoD systems served to confirm and reinforce the findings of ER 97.[16,17]

In ER 97 and SOLAR SUNRISE, DoD systems were proven to be vulnerable to attacks in the cyber domain. The analysis of these attacks showed that DoD had an ineffective system to detect and assess the cyber attacks and was not organized effectively for Information Warfare in the Cyber Domain.[18,19]

ELIGIBLE RECEIVER 97 and SOLAR SUNRISE succeeded in raising awareness of the threat and our corresponding vulnerability in the cyber domain to the highest national levels. In July 1996, in recognition of our growing reliance on and vulnerability in critical information infrastructures, President Clinton signed **Executive Order 13010**. This Executive Order established the **President's Commission on Critical Infrastructure Protection** (PCCIP). The PCCIP's primary task was to develop a comprehensive national strategy and plan for the protection of critical infrastructure from physical and cyber threats.[20]

In October 1997, after fifteen months of analysis, the PCCIP rendered its report, "Critical Foundations - Protecting America's Infrastructures." The report documents the criticality of our cyber-infrastructure and our corresponding vulnerability as follows:

> "The development of the computer and its astonishingly rapid improvements have ushered in the Information Age that affects almost all aspects of American commerce and society. Our security, economy, way of life, and perhaps even survival, are now dependent on the interrelated trio of electrical energy, communications, and computers."[21]

This report detailed the threat, identified our vulnerabilities, and provided recommendations for corrective action. The major findings were: there is a general lack of awareness of our vulnerabilities; our infrastructure is currently vulnerable to physical and cyber attack; our vulnerability is exacerbated by extensive and widespread use of information systems, globalization, and deregulation; a public-private partnership is required because of a shared risk environment due to the interdependent nature of infrastructures, but many legal, social, cultural, and economic impediments exist to establishing a partnership necessary to ensure national protection; and current trends will impact national and economic security if a protection program is not implemented within a three- to five-year window.[22,23]

Subsequent to the PCCIP's report, **Presidential Decision Directive 63** (PDD 63) was published in May 1998 and built upon the recommendations from the PCCIP's October 1997 report. The PDD 63 communicated the President's intent to swiftly eliminate any significant vulnerability of our infrastructure to physical and cyber attack.[24]

The preceding sections reviewed the criticality of the threat, the potentially disastrous impact on our national security, our ever-increasing reliance on our information technology and infrastructure both economically and militarily, and our extreme vulnerability in the area of Information Warfare in the Cyber Domain. We ask ourselves the next question – Are current measures sufficient? Our vulnerability is well known and documented. Our own assessments reveal we are ripe for asymmetrical attack, an aspect that cannot be lost on our potential competitors and adversaries. Next we'll delve further into the complex and inter-connected nature of critical infrastructure, IWCD and national security as addressed in national and DoD policy and guidance.

The White House's, **December 1999, National Security Strategy** (NSS) defines our vital interests as "...- those of broad, overriding importance to the survival, safety, and vitality of our nation." It goes on to state: "Among these are ... the protection of our critical infrastructures - including energy, banking and finance, telecommunications, transportation, water systems, and emergency services - from paralyzing attack."[25] The NSS states our level of commitment to our vital interest as: "We will do what we must to defend these interests, including, when necessary and appropriate, using our military might unilaterally and decisively." Under the heading of Military Activities, the NSS states:

> "We also are committed to maintaining information superiority - the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting and/or denying an adversary's ability to do the same."[26]

In the section on Critical Infrastructure Protection, the NSS unequivocally states:

> "Our national security and economic prosperity rest on a foundation of critical infrastructures, including telecommunications, energy, banking and finance, transportation, water systems, and emergency services. These infrastructures are vulnerable to computer-generated and physical attacks. More than any nation, America is dependent on cyberspace. We know that other governments and terrorist groups are creating sophisticated, well-organized capabilities to launch cyber-attacks against critical American information networks and the infrastructures that depend on them."[27]

This same section also reflects our national commitment to develop and possess the capability to fulfill our national security responsibility through the defense of these critical infrastructures. The commitment includes identification and elimination of significant vulnerabilities and creation of systems to detect and respond effectively to these attacks.[28]

The NSS clearly states the importance of protecting our critical infrastructures in terms of their linkage to our vital national interests. It emphasizes our current and increasing reliance on the cyber domain, our vulnerability, and our commitment to protecting and mitigating this vulnerability for national security.

Our current **National Military Strategy** (NMS), dated September 1997, classifies information warfare as a "special concern" under the heading of Asymmetric Challenges.[29] In addition to identifying information superiority as a key enabler for Joint Vision 2010, the NMS also states: "Joint Vision 2010 rests on the foundations of information superiority and technological innovation."[30] The NMS expands upon the Joint definition of information superiority by specifying:

> "While it is dependent upon superior technology, systems integration, organization and doctrine, it is not an inherent quality but, like air superiority, must be achieved in the battlespace through offensive and defensive information operations."[31]

Department of Defense (DoD) Directive S-3600.1, Subject: "Information Operations (IO)," builds on the policy and guidance found in the NSS and NMS. Reissued on 9 December 1996, it updated applicable policy, definitions and responsibilities for the DoD. The Directive stated:[32]

> -"If deterrence fails, IO seek to achieve U.S. information superiority to attain specific objectives against potential adversaries in time of crisis and/or conflict."
> -"IO are conducted across the full range of military operations. The focus of IO is on decision-making and information-dependent systems including weapons, infrastructure, command and control, computer, and associated network systems."
> -"The goal of IO is to promote freedom of action for U.S forces while hindering adversary efforts."

DoD Directive S-3600.1 follows the intent of the NSS by stating: "...the DoD shall be organized, trained, equipped, and supported to plan and execute Information Warfare against specific adversaries."[33] Additionally, the Directive links to the Joint arena by directing that the Chairman of the Joint Chiefs of Staff "...establish doctrine to facilitate the integration of IO concepts into Joint operations."[34]

Joint Vision 2020 (JV 2020), released in May 2000, is intended to build on and refine the previously published Joint Vision 2010 (JV 2010).[35] It gives direction to how the military must change to meet the challenges of the future. As with JV 2010, the success of JV 2020 rests on the foundation of information superiority. Joint Vision 2020 states:

> "The transformation of the Joint force to reach full spectrum dominance rests upon information superiority as a key enabler and our capacity for innovation."[36]

The policies addressing the vulnerability, imminent threat, criticality, and essentiality of actions required for Information Warfare in the Cyber Domain are clear and consistent. This consistency is articulated and evidenced in Presidential Executive Orders and Directives, the National Security Strategy, the National Military Strategy, DoD policy, and Joint Vision 2020.

Joint Pub 3-13 (JP 3-13), Joint Doctrine for Information Operations, published 9 October 1998, represents the current doctrine for Information Operations in joint operations.[37] It does exceptionally well at portraying a highly complex, multi-faceted subject that is rapidly evolving. Joint Pub 3-13 provides a solid doctrinal foundation in order to foster common understanding. It accomplishes this by: establishing common terminology and definitions; identifying responsibilities for planning, coordinating, integrating and de-conflicting joint IO; fostering thought towards controlling and using the cyber domain; addressing information operations as a method, weapon, or tool; and providing operational guidance for the integration and synchronization of IO as part of combatant commanders' plans and operations at the tactical, operational, and strategic levels of war.

However, if one were searching for guiding principles, they are addressed only intermittently throughout JP 3-13. For example, of the nine accepted principles of war normally embodied in Joint doctrine, offensive and objective were addressed briefly under offensive IO,[38] unity of command was only mentioned in terms of the basis for establishing relationships during IO planning,[39] and security only as the derived basis for defensive IO.[40]

Perhaps this treatment of the principles of war by JP 3-13 is a reflection of the restricting nature of the Joint definition of Information Operations: "actions taken to affect adversary information and information systems while defending one's own information and information systems."[41] While adequate in terms of current thinking about Information Operations, this definition may have been limiting to the boundaries of conceptual and doctrinal development.

Joint Pub 3-13 does take us to the important first step of promoting a standard of how to think about IO. But as noted previously, the cyber domain can also be viewed as its own battlespace. Previously, our concept of battlespace only encompassed the domains of ground, sea, and aerospace, but now, has been expanded to include the cyber domain. Like that of the ground, sea, and aerospace, the cyber domain is a battlespace that must be controlled and can be exploited in order to ensure operational freedom of action and the achievement of objectives.

Both the sea and aerospace domains required adaptations to the fundamental principles of war and required development of new principles unique to the pursuit of sea and aerospace control. We have now entered another domain, another battlespace. Again, as in the past, to be successful, combatants must divine the implications and impacts of technological change, and develop and apply ***the*** correct doctrine. The next section provides, for consideration, a suggested alternative approach for further doctrinal development.

Example of One Possible Approach for Further Doctrinal Development.

The introductory sections spoke of advances in technology and the relationship to our national security. The question remains as to whether we have developed ***the*** doctrine for this new technology that ensures our desired ends (national security). Only the future can tell. We must apply thought in an attempt to divine the correct ways (doctrine) to use these new means (technology) to achieve our desired ends. We must continually apply mental energy in order to learn, adapt, and anticipate correctly. The following is provided for general consideration; it is an example of **an** approach, not **the** prescribed approach, for further doctrinal development. Ideally, it will serve as food for thought and reflection.

As stated earlier, IWCD departs conceptually from IO and NCW on several points. First, IWCD views cyber superiority (or supremacy) as the essential element or condition to set, sine qua non for operational success. Second, that IWCD can represent the weapon of choice, not just limited to the role of an enabler. And third, IWCD can by itself bring about conflict resolution or termination in certain circumstances.

Our intention is to introduce ***an*** approach of doctrinal development. In this case, purposefully applying the nine fundamental principles of war "the enduring bedrock of U.S. military doctrine" in a clear, unambiguous, and succinct manner to IWCD. We start with the view that the environment has changed. There are new technological means available, and doctrine must be developed to match these changes. We then use the fundamental principles of war as the foundation for building new operational doctrine for IWCD. By construct, we'll first present the fundamental principles of war from Joint Pub 3.0, Doctrine for Joint Operations; second, we'll show the articulation of these principles from the USAF's basic doctrinal manual, AFDD-1; and third, we'll synthesize the principles of war and the USAF doctrine into a rudimentary application to IWCD. Finally, we'll present examples describing how we may operationally use these synthesized principles and new concepts of IWCD.

U.S. Air Force doctrine was selected for this approach because it offers a rich source of thought, perspective, and potential direction. As our youngest service component, the USAF, while rooted in history and the fundamentals of warfare, has a culture of taking new technology (flight) applying it to a medium (aerospace) and continuously developing successful concepts and doctrine. Their approach to doctrinal development is reflected in their basic doctrinal manual:

> "...Air Force doctrine must draw together the lessons of history, the vectors of technology, and our insights about the future. As our experience in air and space warfare has evolved, however, these historic principles must now be viewed in light of modern air and space capabilities. ...we must debate and refine these ideas for the future."[42]
>
> —Air Force Basic Doctrine, GEN Michael E. Ryan, USAF Chief of Staff

Nine Fundamental Principles of War:[43,44]

Objective:

Basic Joint principle:

~...to direct every military operation toward a clearly defined, decisive, and attainable objective.

~...the objective of combat operations is the destruction of the enemy armed forces' capabilities and will to fight.

~ Each operation must contribute to strategic objectives.

USAF's articulation:

* Success in military operations demands that all efforts be directed toward the achievement of common aims.

* In application, this principle refers to unity of effort.

*...holds that political and military goals should be complementary and clearly articulated.

*...forces do not normally need to sequentially achieve tactical objectives first before pursing operational or strategic objectives.

*...can pursue tactical, operational, or strategic objectives, in any combination, or all three simultaneously.

*...shapes priorities to allow...forces to concentrate on theater or campaign priorities and seeks to avoid the siphoning of force elements to fragmented objectives.

Produce a synthesized application of:

Integrate IWCD operations toward accomplishment of clearly defined military and political goals and objectives through their orchestration in time, space, and domains. IWCD conducts and supports decisive operations across the entire tactical, operational, and strategic spectrum of conflict through speed, combinations of simultaneity and sequencing, and precision. The objective of IWCD is to deny, negate or destroy an adversary's ability and will to fight.

Offensive:

Basic Joint principle:

~...purpose of an offensive action is to seize, retain, and exploit the initiative.

~ Offensive action is the most effective and decisive way to attain a clearly defined objective.

~...the means by which a military force seizes and holds the initiative while maintaining freedom of action and achieving decisive results.

~ Commanders adopt the defensive only as a temporary expedient and must seek every opportunity to seize the initiative.

~ An offensive spirit must therefore be inherent in the conduct of all defensive operations.

USAF's articulation:

*...forces are best used as an offensive weapon.

*...success in war is generally attained only while on the offensive.

*...a well-planned and executed...attack is extremely difficult to completely stop.

*...defenders often require more forces to defend...than the attacker requires to strike.

*...immediately seize the initiative [through the offensive].

*...cause the enemy to react rather than act, deny the enemy the offensive, and shape the remainder of the conflict.

Produce a synthesized application of:

Employ IWCD to seize, retain, and exploit the initiative through its inherent offensive capability. The offensive predominates in IWCD. The ubiquitous nature of IWCD causes the opponent to expend resources defending everywhere and reacting while the attacker pursues his objectives through freedom of action. Offensive IWCD is the most effective method to deny an adversary the initiative and freedom of action.

Mass:

Basic Joint principle:

~ The purpose of mass is to concentrate the effects of combat power at the place and time to achieve decisive results.

~ To achieve mass is to synchronize appropriate joint force capabilities where they will have [a] decisive effect in a short period of time.

~ Massing effects, rather than concentrating forces...to achieve decisive results and minimize human losses and waste of resources.

USAF's articulation:

*...to launch an attack from widely dispersed locations and mass combat power at the objective.

*...mass is an effect ...achieve[d] through efficiency of attack.

*...speed, range, and flexibility...complemented by the accuracy and lethality of precision weapons...achieve mass faster.

Produce a synthesized application of:

Achieve the massed, concentrated effects of IWCD, at the decisive places and times through its capability to launch precise, synchronized, worldwide attacks through distributed operations. IWCD employs its inherent speed, flexibility, and versatility during distributed attacks in time, space, and medium to achieve massed, synchronized, and concentrated effects. Mass the effects of IWCD to paralyze, overwhelm, and control an adversary.

Economy of force:

Basic Joint principle:

~ The purpose of economy of force is to allocate minimum essential combat power to secondary efforts.

~...is the judicious employment and distribution of forces.

USAF's articulation:

*...rational use of force by selecting the best mix of combat power.

*...requires clearly articulated objectives and priorities.

*...recommends against "overkill" by guarding against unnecessary force.

*...particularly relevant in military operations other than war in which excessive force can destroy the gaining and maintaining ...of legitimacy and support for an operation.

Produce a synthesized application of:

Achieve Economy of Force through the precision and speed inherent in IWCD. IWCD capabilities are ideal for tailoring calculated action towards accomplishment of discrete operations or limited objectives. The ability to modulate IWCD is of particular value when guarding perceptions of proportionality, legitimacy, and collateral impact. Precise use of IWCD allows friendly forces the ability to control and manage the affects on an adversary.

Maneuver:

Basic Joint principle:

~ The purpose of maneuver is to place the enemy in a position of disadvantage through the flexible application of combat power.

~ Effective maneuver keeps the enemy off balance and thus protects the friendly force.

~ It contributes materially in exploiting success, preserving freedom of action, and reducing vulnerability by continually posing new problems for the enemy.

USAF's articulation:

*...maneuver forces the enemy to react, allows the exploitation of successful friendly operations, and reduces our vulnerabilities.

*...the ability to integrate a force quickly and to strike directly at an adversary's strategic or operational center of gravity.

*...allows engagement almost anywhere, from any direction, thus forcing the adversary to be on guard everywhere.

*...simultaneous application of mass and maneuver.

Produce a synthesized application of:

Use the ubiquity and speed of IWCD to achieve tactical, operational, and strategic maneuver across time, space, and domain. IWCD maneuver must be governed and measured by its affects on the adversary. That is, use IWCD to keep the adversary at a disadvantage, forced to constantly react to our initiative, remaining constantly off balance, lacking freedom of action, and vulnerable at his most critical points. IWCD maneuver protects our vulnerabilities and directs decisive effects against the adversary's center(s) of gravity.

Unity of Command:

Basic Joint principle:

~ The purpose of unity of command is to ensure unity of effort under one responsible commander for every objective.

~ Unity of effort – coordination through cooperation and common interests – is an essential complement to unity of command.

USAF's articulation:

*...all efforts should be coordinated towards a common objective.

*...must be preserved in order to ensure common focus and mutually supporting actions.

*...best achieved by vesting a single commander with the authority to direct all force employment.

*...central command and control is essential to effectively fuse these capabilities.

Produce a synthesized application of:

Achieve and maintain operational Unity of Command and effort by designating a single functional commander for IWCD. Give this functional commander the responsibility to provide centralized direction and control for the decentralized execution of IWCD operations. Exploit the full potential of IWCD by the effective fusing, synchronization, and orchestration of each service's capabilities in support of IWCD operations. Unity of Command provides an advantage over an adversary through greater efficiency and effectiveness and thus the ability to overwhelm and control.

Security:

Basic Joint principle:

~ The purpose of security is to never permit the enemy to acquire [an] unexpected advantage.

~ Security enhances freedom of action by reducing friendly vulnerability to hostile acts, influence, or surprise.

~ Application of this principle includes prudent risk management, not undue caution.

USAF's articulation:

*...requires that friendly forces and their operations be protected from enemy action that could provide the enemy with [an] unexpected advantage.

*...gaining or maintaining control of...mediums provides friendly forces a significant advantage.

*...security from enemy intrusion, concealing friendly capabilities and intentions while allowing our forces the freedom to gather information on the adversary.

*...information technology can directly or indirectly affect national or group leadership, population, and infrastructure, bypassing direct military confrontation.

*...whoever has the best ability to gain, defend, exploit, and attack information, and deny the same capabilities to an opponent has a distinct strategic advantage.

Produce a synthesized application of:

Use IWCD to attain and maintain security. Gain cyber supremacy through IWCD in order to ensure undisputed control, freedom of action, and protection of friendly forces from intrusion and attack. Conduct operations to deny the adversary security and sanctuary. The initiative and an offensive orientation must be maintained even in defensive operations.

Surprise:

Basic Joint principle:

~ The purpose of surprise is to strike the enemy at a time and place or in a manner for which it is unprepared.

~ Factors contributing to surprise include speed of decision-making, information sharing, and force movement; effective intelligence; deception; application of unexpected combat power; OPSEC; and variations in tactics and methods of operation.

USAF's articulation:

*...leverages the security principle.

*...speed and range...coupled with...flexibility and versatility, allow...[achievement of] surprise

*...choice of time and place of assault rest with [attacking commander].

*...provide shock and surprise without unnecessarily exposing massed friendly forces.

*...can enhance and empower [other] forces to achieve surprise.

*...seizing the initiative through surprise.

Produce a synthesized application of:

Achieve surprise in IWCD operations by taking actions at an unexpected time, place, and manner. Degrade and undermine the adversary's ability to resist by generating or reinforcing conditions of shock, disorientation, and confusion. Use the inherent speed, flexibility, and versatility of IWCD to seize and maintain the initiative and freedom of action in order to achieve decisive results. Use IWCD to keep an adversary constantly off balance, unsure, and paralyzed.

Simplicity

Basic Joint principle:

~ The purpose of simplicity is to prepare clear, uncomplicated plans and concise orders to ensure thorough understanding.

~...minimize misunderstanding and confusion.

~...allows better understanding and execution planning...

~ Simplicity and clarity of expression greatly facilitate mission execution in the stress, fatigue, and other complexities of modern combat ...

USAF's articulation:

*...avoiding unnecessary complexity in organizing, preparing, planning, and conducting military operations.

*...simple guidance allows...the freedom to creatively operate within their battlespace.

*...straightforward plans and unambiguous organizational and command relationships are essential.

Produce a synthesized application of:

Seek simplicity in IWCD operations by counteracting the potential complexity of technology through clear and unambiguous unity of command and effort (e.g., organizational and command relationship), simple plans and guidance, central objective focus, and articulation of mission intent. Simplicity is particularly critical when operating in a distributed manner in time, space, and medium while at the same time seeking massed, synchronized, and concentrated effects. Simplicity allows greater velocity, effectiveness, and efficiency relative to an adversary.

This possible approach to doctrinal development takes the basic principles of war, integrates the USAF's doctrinal interpretation of each principle, and synthesizes them into principles for IWCD. The preceding was a very rudimentary example of just one method Joint doctrine developers may choose to take.

Examples of the Operational Use of Synthesized Principles:

Building upon our nine synthesized principles of war and three new premises of IWCD (i.e., establishment of cyber supremacy is essential for success, IWCD can be the weapon of choice, and IWCD can itself bring about conflict resolution) we conclude this section with **examples of how we may operationally use these synthesized principles.** The basis for these examples are the USAF's basic Air and Space Power functions of Counterair (which includes both Offensive and Defensive Counterair), Counterspace (which includes Offensive and Defensive Counterspace), Counterland (which includes Interdiction), Countersea, Strategic Attack, Counterinformation, and Command and Control. The Air Force defines basic functions as their fundamental ways to shape and control battlespace to achieve their tactical, operational and strategic objectives.[45]

-Establish and maintain cyber superiority (or supremacy). Never cede the initiative or control of a battlespace to an adversary. This should be the first priority for any operation. One of the essential objectives of IWCD is to gain, maintain, and exploit control of the medium [domain], i.e., allow friendly forces to exploit their capabilities, while negating the enemy's ability to do the same.

-Achieve domain superiority by aggressive offensive IWCD operations. Offensive operations are the most effective, efficient, and decisive method to bring about the rapid and decisive achievement of objectives. IWCD operations are intended to destroy, neutralize, disrupt, deceive, deny, degrade, manipulate, or limit the adversary's systems or the information they provide as close to its source as possible and at times and places of our choosing. Offensive operations protect friendly forces and vital interests by destroying or neutralizing the adversary's offensive capabilities before they can be employed against us.

-Establish and maintain the desired degree of cyber superiority by executing focused, orchestrated, and synchronized decisive IWCD operations in order to destroy or neutralize the adversary's forces and capabilities. IWCD operations best achieve optimal effects and effectiveness through centralized control and decentralized execution. The intent of these operations is to enable our unrestricted use of otherwise contested cyberspace and to disable the adversary's offensive cyber capabilities in order to secure friendly forces from threats or actual attacks and to achieve our objectives.

-Achieve strategic objectives by directing IWCD operations with the intent of directly affecting the adversary's center of gravity (COG). Correctly determined, a COG should represent the source(s) from which the enemy derives its freedom of action, physical strength, or will to fight. Ideally, a successful IWCD operation against an adversary's COG would rapidly achieve a decisive effect upon the adversary thus securing our strategic goals while avoiding unnecessary loss of life and national treasure.

-Direct IWCD operations towards gaining and maintaining freedom of action and protection of friendly forces. IWCD may include such operational missions as interdiction (i.e., diversion, disruption, delaying, interception, and/or destruction of enemy information before it can be used), suppression, jamming, blockage, canalization, deception, denial, and degradation. Some of the desired effects of IWCD on the adversary are: systemic failures, physical and psychological paralysis, confusion, defeat of an adversary's plans, infliction of unacceptable losses on attacking forces and capabilities, dissolution of unity, and capitulation. Cause the rapid termination of conflict by eliminating the adversary's will and ability to continue to fight.

-Seize and maintain the initiative in defensive IWCD operations by preemptively defeating the adversary's offensive plan and neutralizing his ability to attack our vulnerabilities or exercise freedom of action. These operations consist of active and passive measures to reduce vulnerability and increase survivability of friendly forces and the information they provide. Defensive IWCD operations are intended to defend friendly forces and their cyber space, material, and infrastructure from attack. Specific missions are detection, identification, interception, interdiction, and preemptive, preparatory, and counter strikes. Additional tasks may include designing survivability features into systems and information architecture, satellite maneuver, tracking, emission control, and deception.

The preceding serve only as examples. They are adaptations from the doctrine associated with the basic USAF functions listed above. They are rooted in the principles of war and the three underlying premises that establishment of cyber supremacy is essential for success, IWCD can be the weapon of choice, and IWCD can itself bring about conflict resolution. These examples represent taking existing thought, critically analyzing the implications of a changing environment, and then adapting, changing, or developing thought with the goal of deriving ***the*** correct doctrine for the new environment.

Summation.

We started with the premise that Information technology, particularly in the cyber domain, is rapidly advancing. As our reliance on this technology increases, so too does our vulnerability in terms of national security. In the preceding sections we have seen the linkage to our nation interests and survival, the nature of the threat and our vulnerability, and the thought thus far in policy, guidance, vision and doctrine. Recognizing this situation, we derived the corollary that it is imperative to continue the development of operational doctrine for Information Warfare in the Cyber Domain.

The advancements in computing power, telecommunications systems, and the global interconnectivity of these systems require basic changes in the treatment and approach to Information Warfare and its new battlespace – the cyber domain. As a step towards this goal, we looked at a new paradigm for the principles of war given three premises: 1) establishment of cyber supremacy is essential for operational success, 2) IWCD can be the weapon of choice for future decision-makers, and 3) IWCD can itself bring about conflict resolution in certain situations. Next, we looked at a possible approach to doctrinal development that took the nine principles of war, integrated the USAF's doctrinal interpretation of each principle and synthesized them into principles for IWCD. Finally, we looked at some examples of how to employ the synthesized principles and three new premises of IWCD in operational doctrine.

Doctrinal development must be made a top priority. This paper presented an example of ***a*** possible approach to further doctrinal development using the nine principles of war as a framework. There are many other methods. The intent is to spur further thought and progress towards developing ***the*** correct doctrine for our nation. New approaches, paradigms, and doctrine are required to allow our control and unrestricted use of this new medium in order to achieve tactical, operational, and strategic objectives and ultimately ensure our national security.

If we are to fight and win in the battlespace envisioned by JV 2020, we must act decisively in order to achieve and ensure our superiority in terms of Information Warfare in the Cyber Domain. We must develop Joint and Service doctrine that keeps pace with technological advancement in order to harness IWCD's capability and guard against its use by an adversary. IWCD should not be an afterthought or add-on to doctrine.

Change is upon us, but our responsibilities for national security remain constant. We must develop the necessary concepts and doctrine for the new technology in order to fulfill our responsibilities.

> "Even as we adjust to face a changed security environment, our goals remain firm: We must protect America's interest. We must deter aggression. We must support the peaceful resolution of disputes, and most important, we must be ready to intervene or respond to a conflict and win decisively."[46]
>
> —GEN Henry H. Shelton, Chairman of the Joint Chiefs of Staff

WORD COUNT = 7141

ENDNOTES

[1] Department of Defense, Dictionary of Military and Associated Terms, Joint Publication 1-02 (Washington, D.C.: U.S. Department of Defense, 10 June 1998), 142.

[2] Chairman of the Joint Chiefs of Staff, Joint Vision 2020, (Washington, D.C.: U.S. Department of Defense, May 30, 2000), 2-3, 10, 3.

[3] Eliot A. Gooch and John Gooch, Military Misfortunes: The Anatomy of Failure in War, (New York.: Vintage Books, Random House, 1990), 197-230.

[4] Department of the Air Force, Information Operations, USAF Doctrine Document 2-5 (Washington, D.C.: Department of the Air Force, August 1998), Foreword.

[5] Assistant Secretary of Defense, Command, Control, Communications, and Intelligence, Information Superiority: Making the Joint Vision Happen (Washington, D.C.: U.S. Department of Defense, undated), 3.

[6] Department of Defense, Joint Doctrine for Information Operations, Joint Publication 3-13 (Washington, D.C.: U.S. Department of Defense, 9 October 1998), Glossary.

[7] David S. Alberts, John J. Garstka, and Frederick P. Stein, Network Centric Warfare: Developing and Leveraging Information Superiority (Washington, D.C.: DoD C4ISR Cooperative Research Program, 1999), 2.

[9] Martin C. Libicki, The Mesh and The Net: Speculations on Armed Conflict in a Time of Free Silicon (Washington, D.C.: National Defense University, August 1995), 68,80,81. Libicki's ideas formed the genesis of the three new premises.

[9] Winn Schwartau, CyberShock: Surviving Hackers Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption (New York: Thunder's Mouth Press, 2000), 348.

[10] Ibid., 394.

[11] U.S. Army War College, Selected Readings, Course 4, Volume IV, Information Assurance-the Achilles' Heel of Joint Vision 2010?, (Carlisle Barracks: U.S. Army War College, AY 2001), 25-70-73.

[12] The Joint Staff, Information Assurance: Legal, Regulatory, Policy and Organizational Considerations, (Washington D.C.: U.S. Department of Defense, 25 August 1999), 1-2.

[13] Ibid.

[14] The no-notice Joint Staff exercise ELIGIBLE RECEIVER 97 (ER97) was designed to test the effect of information warfare attacks in the cyber domain on the Department of Defense (DoD)'s planning and crisis action systems. The exercise participants were the Department of Defense (DoD), the Joint Staff, five Unified

Commands, the National Security Agency, the Defense Information Systems Agency, the National Security Council, the Defense Intelligence Agency, the Central Intelligence Agency, the Federal Bureau of Investigation, the National Reconnaissance Office, the Department of State, the Department of Justice, and the Department of Transportation.

[15] Information Assurance-the Achilles' Heel of Joint Vision 2010?, 25-71.

[16] Ibid., 25-72.

[17] These teenagers had followed an attack profile of first probing for vulnerability, then exploiting that vulnerability by emplacing a program to gather the data they desired, and returning at a later time to retrieve the collected data.

[18] Information Assurance-the Achilles' Heel of Joint Vision 2010?, 25-72.

[19] Reports from the General Accounting Office (GAO) also provide findings and recommendations that confirm DoD's vulnerabilities in information security. In a 26 August 1999 report to Secretary of Defense William S. Cohen:
"Indeed, its [DoD's] warfighting capability depends upon computer-based telecommunications networks and information systems. In recent years, numerous internal and external evaluations have identified weaknesses in information security that could seriously jeopardize DoD's operations and compromise the confidentiality, integrity, or availability of sensitive information."
"Serious weaknesses in DoD information security continue to provide both hackers and hundreds of thousands of authorized users the opportunity to modify, steal, inappropriately disclose, and destroy sensitive DoD data."

The report also made reference to GAO report 96-84, titled "Information Security: Computer Attacks at DoD Pose Increasing Risks," dated May 22, 1996, which stated that external attacks on DoD computer systems were a serious and growing threat. The primary thrust of the recommendations of both reports was: to empower DoD" to establish a comprehensive DoD-wide information security program; ensure DoD-wide continuity, consistency, and compliance with this information security program; and establish a system to periodically report progress in improving controls over information security.

[20] Information Assurance: Legal, Regulatory, Policy and Organizational Considerations, ES-1, 2.

[21] U.S. Army War College, Selected Readings, Course 4, Volume IV, The President's Commission on Critical Infrastructure Protection, Report Summary: Critical Foundations, Thinking Differently, (Carlisle Barracks: U.S. Army War College, AY 2001), 25-31.

[22] Robert T. Marsh, Critical Foundations: Protecting America's Infrastructures, (Washington, D.C.: President's Commission on Critical Infrastructure Protection, October 1997), vii-xii.

[23] The PCCIP's recommendations called for: new thinking; establishment of a national organizational structure with specific responsibilities to give national focus and direction (to our efforts); establishment of a public-private partnership that fosters

cooperation, responsibility, and sharing of information; and development and implementation of two plans designed to accomplish these objectives. The new national organizational structure created the position of National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism; established the Critical Infrastructure Assurance Office (CIAO) and the National Infrastructure Protection Center. The National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism is responsible for execution of the infrastructure protection program. The Coordinator reports to the President through the National Security Advisor. Specific responsibilities of the position include advising the President on applicable budget matters and ensuring coordination for policy development, implementation and crisis management within the area of security, infrastructure protection, and counter-terrorism. The Critical Infrastructure Assurance Office is a multi-agency manned organization responsible for overall integration of the National Infrastructure Assurance Plan (NIAP). The National Infrastructure Protection Center NIPC is a multi-agency manned organization responsible to facilitate and coordinate the federal government's threat assessment, warning, vulnerability, investigation (law enforcement), and response.

[24] William J. Clinton, Presidential Decision Directive/NSC-63: Critical Infrastructure Protection, (Washington, D.C.: The White House, May 22, 1998). . The directive established national goals to achieve an initial operating capability to protect our critical infrastructure by the year 2000 and the full capability to protect critical infrastructures by 2003. Specifically, PDD 63 established a national organizational structure, called for a public-private partnership and called for the creation of two sets of plans. The first set would outline each Federal agency's plan to protect its portion of the Federal infrastructure. The second set would be a comprehensive National Infrastructure Assurance Plan that would call on the public and private sector to develop a partnership and devise a plan to incorporate protection of all areas of public and private infrastructure.

[25] William J. Clinton, A National Security Strategy for a New Century, (Washington, D.C.: The White House, December 1999), 1.

[26] Ibid., 12.

[27] Ibid., 17.

[28] Ibid., 17-18.

[29] Chairman of the Joint Chiefs of Staff, National Military Strategy of the United States of America, (Washington, D.C.: U.S. Department of Defense, September 1997), 9.

[30] Ibid., 17.

[31] Ibid., 18.

[32] Department of Defense, Information Operations (IO) (U), DoD Directive S-3600.1 (Washington, D.C.: U.S. Department of Defense, 9 December 1996), 1-3.

[33] Ibid., 3.

[34]Ibid., 7.

[35]Department of Defense, Joint Vision 2020, (Washington D.C., U.S. Government Printing Office, June 2000), 1.

[36]Ibid., 10.

[37]Joint Pub 3-13, II-1.

[38]Ibid., II-1.

[39]Ibid., V-3.

[40]Ibid., III-1.

[41]Ibid., vii.

[42]Department of the Air Force, Air Force Basic Doctrine, USAF Doctrine Document 1 (Washington, D.C.: Department of the Air Force, September 1997), Foreword.

[43]Ibid., This represents a brief articulation of the nine principles of war by the USAF.

[44]Department of Defense, Doctrine for Joint Operations, Joint Publication 3-0 (Washington, D.C.: U.S. Department of Defense, 1 February 1995), Appendix A. This represents a brief articulation of the nine principles of war as found in Joint doctrine.

[44]USAF Doctrine Document 1, 46-53.

[46]GEN Henry H. Shelton, "The National Military Strategy And Joint Vision 2020," Army (January 2001): 7-9.

BIBLIOGRAPHY

Alberts, David S., John J. Garstka, and Frederick P. Stein. Network Centric Warfare: Developing and Leveraging Information Superiority. Washington, D.C.: DoD C4ISR Cooperative Research Program, 1999.

Assistant Secretary of Defense. Command, Control, Communications, and Intelligence, Information Superiority: Making the Joint Vision Happen. Washington, D.C.: U.S. Department of Defense, undated.

Chairman of the Joint Chiefs of Staff. National Military Strategy of the United States of America. Washington, D.C.: U.S. Department of Defense, September 1997.

Chairman of the Joint Chiefs of Staff. Joint Vision 2020. Washington, D.C.: U.S. Department of Defense, 30 May 2000.

Clinton, William J. A National Security Strategy for a New Century. Washington, D.C.: The White House, December 1999.

Clinton, William J. Presidential Decision Directive/NSC-63. Critical Infrastructure Protection. Washington, D.C.: The White House, 22 May 1998.

Gooch, Eliot A. and John Gooch. Military Misfortunes: The Anatomy of Failure in War. New York.: Vintage Books, Random House, 1990.

The Joint Staff. Information Assurance: Legal, Regulatory, Policy and Organizational Considerations. Washington, D.C.: U.S. Department of Defense, 25 August 1999.

Libicki, Martin C. The Mesh and The Net: Speculations on Armed Conflict in a Time of Free Silicon. Washington, D.C.: National Defense University, August 1995.

Marsh, Robert T. Critical Foundations: Protecting America's Infrastructures. Washington, D.C.: President's Commission on Critical Infrastructure Protection, October 1997.

Schwartau, Winn. CyberShock: Surviving Hackers Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption. New York: Thunder's Mouth Press, 2000.

Shelton, Henry H. (GEN). "The National Military Strategy And Joint Vision 2020." Army (January 2001): 7-9.

U.S. Army War College. Selected Readings, Course 4, Volume IV, Information Assurance-the Achilles' Heel of Joint Vision 2010?. Carlisle Barracks: U.S. Army War College, AY 2001.

U.S. Army War College. Selected Readings, Course 4, Volume IV, The President's Commission on Critical Infrastructure Protection, Report Summary: Critical Foundations, Thinking Differently. Carlisle Barracks: U.S. Army War College, AY 2001.

U.S. Department of the Air Force. Air Force Basic Doctrine, USAF Doctrine Document 1. Washington, D.C.: U.S. Department of the Air Force, September 1997.

U.S. Department of the Air Force. Information Operations. USAF Doctrine Document 2-5. Washington, D.C.: U.S. Department of the Air Force, August 1998.

U.S. Department of Defense. Dictionary of Military and Associated Terms. Joint Publication 1-02. Washington, D.C.: U.S. Department of Defense, 10 June 1998.

U.S. Department of Defense. Doctrine for Joint Operations. Joint Publication 3-0. Washington, D.C.: U.S. Department of Defense, 1 February 1995.

U.S. Department of Defense. Information Operations (IO) (U). DoD Directive S-3600.1. Washington, D.C.: U.S. Department of Defense, 9 December 1996.

U.S. Department of Defense. Joint Doctrine for Information Operations. Joint Publication 3-13. Washington, D.C.: U.S. Department of Defense, 9 October 1998.